

Formalization of scenarios for testing automated driving functions

Hardi Hungar
Institute of Transportation Systems
German Aerospace Center (DLR)

This research was partially funded by the German Federal Ministry for Economic Affairs and Energy, Grant No. 19A15012F (PEGASUS), based on a decision by the Parliament of the Federal Republic of Germany. The responsibility for the content lies with the author.

A large, high-resolution image of the Earth from space occupies the right half of the slide. It shows a curved horizon with a blue sky, white clouds, and green landmasses. The text "Knowledge for Tomorrow" is overlaid on the lower right portion of this image.

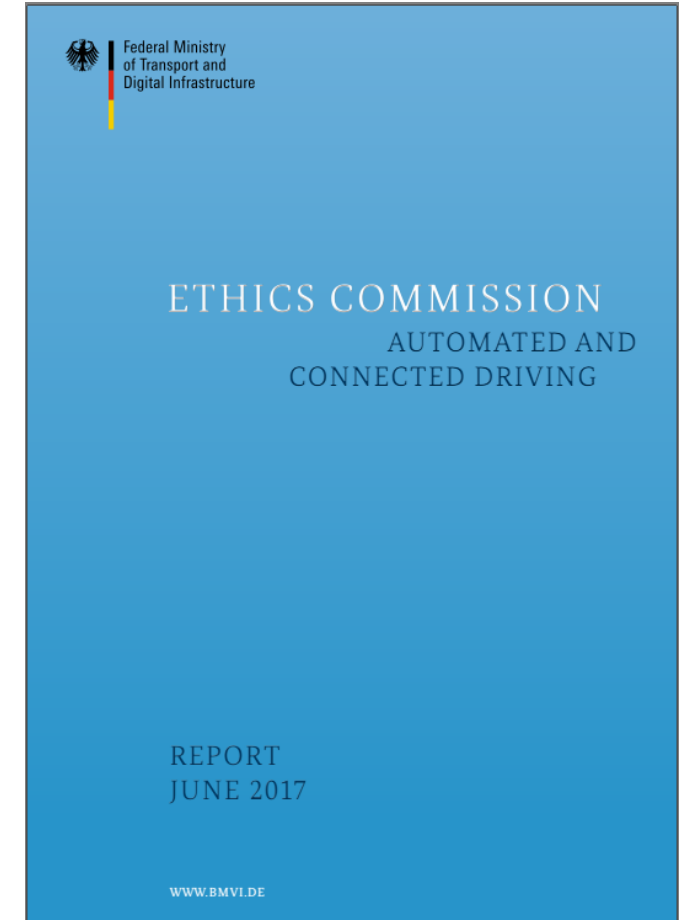
Knowledge for Tomorrow

Safety target for automated driving

Ethics Commission on Automated Driving set up by the German Federal Ministry of Transport and Digital Infrastructure (BMVI)

Fully automated driving systems:

1. [...] [Their] primary purpose [...] is to **improve safety** for all road users.
2. [...] produce at least a diminution in harm compared with human driving, in other words a **positive balance of risks**.

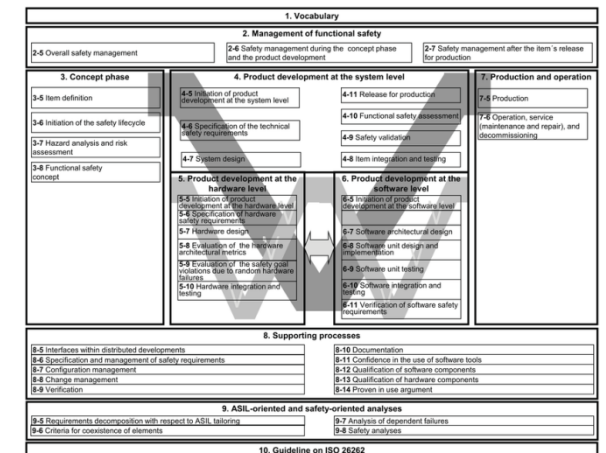


The “standard” approach – ISO 26262

- **ISO 26262:** Standard „Road Vehicles – Functional Safety“ for developing systems with electronic elements (additional considerations: SOTIF ISO/WD PAS 21448)
 - Risk-based approach to safety

Similar to insurance risk calculation

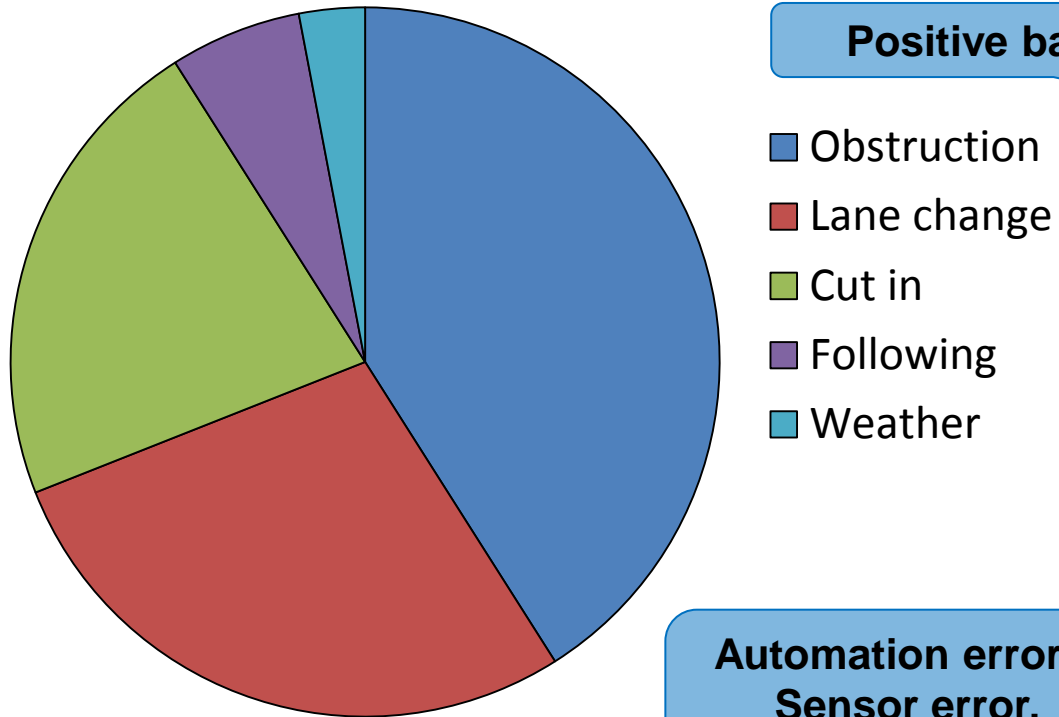
- Risk $\approx \sum_{h \in H} E_h * C_h * S_h$
 - H : Set of harmful events h
 - E : probability of occurrence (precisely: expected number per time unit)
 - C : controllability (here: probability of *not* avoiding an accident)
 - S : severity of event (injuries, fatalities)



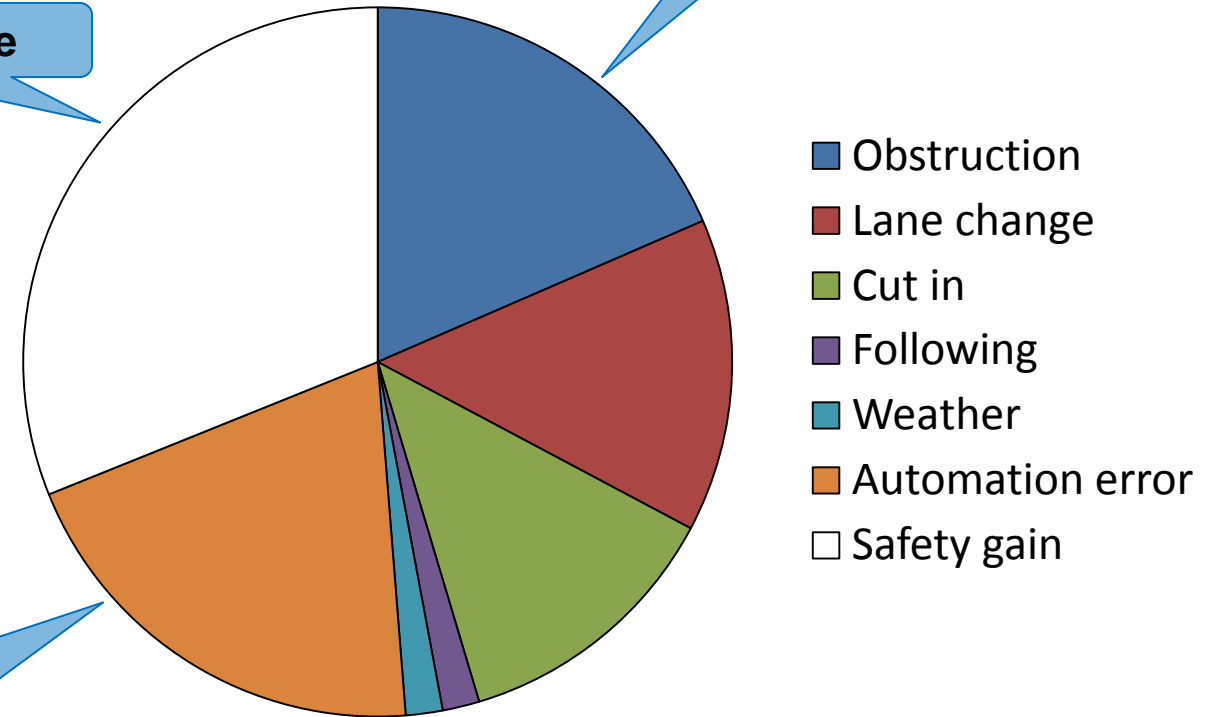
ISO 26262, Overview figure

Safety target (illustration)

Risk chart human driver



Risk chart automation



Positive balance

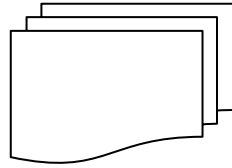
Automation errors:
Sensor error,
misinterpretation etc.

Improvement in
each category



Risk assessment (commonly applied procedure)

- List all hazards
- Determine
 - Exposure
 - Criticality
 - Severity
- Sum up for overall risk



Hazard	E	C	S	Risk
Obstruction				
Lane change				
Cut in				
Cut through				
Overtaking				
Lane violation				
...				
...				
Sum				



Systematic computation of risk chart

1. Derive all potentially critical evolutions
2. Formalize the evolutions in precise descriptions of classes of evolutions
3. Exhaustive testing of evolution classes
 1. Derive concrete instantiations of a class
 2. Test concrete instances
 3. Identify critical instances
4. Analyze the critical instances
 1. Detailed evaluation
 2. Aggregate in risk chart

Functional scenarios

Logical scenarios

Concrete critical scenarios

Risk chart

Hazard	E	C	S	Risk
Obstruction				
Lane change				
Cut in				
Cut through				
Overtaking				
Lane violation				
...				
...				
Sum				

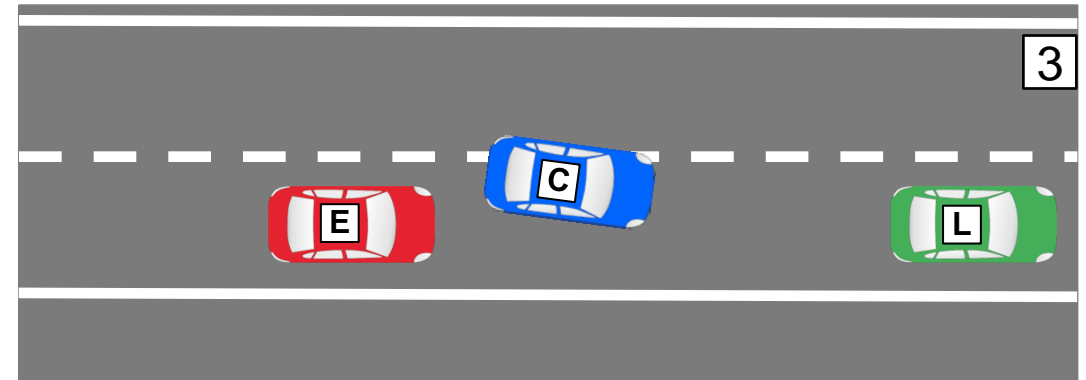
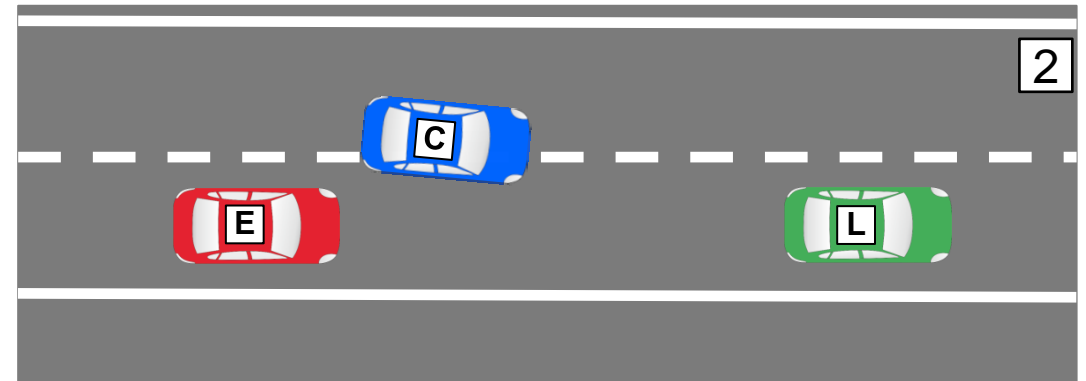
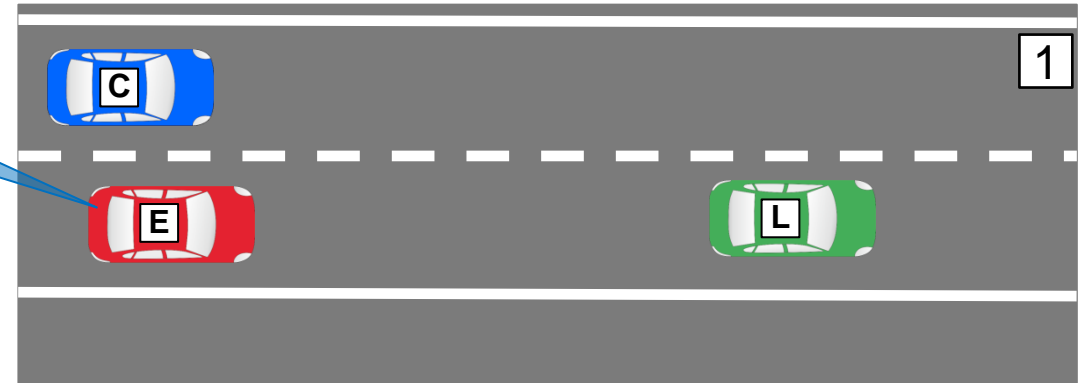


Functional scenario “cut in”

- Rough storyboard of a cut-in evolution
- Sequence of events
 - **C** is approaching on left lane
 - **C** overtakes **E**
 - **C** changes to right lane in front of **E**
- Parametrizing and varying over discrete variants yields the concrete instantiations of a “cut-in”

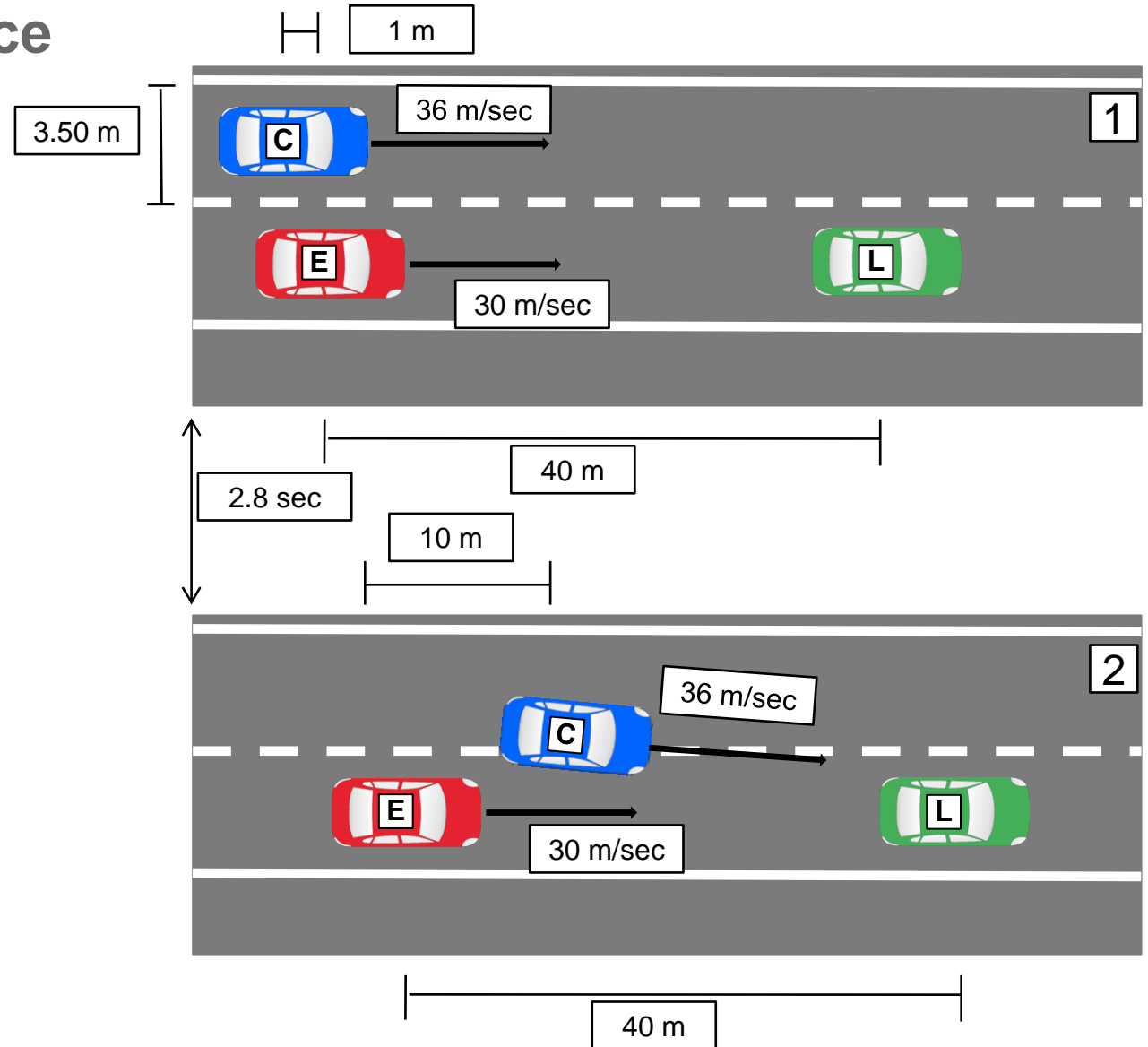
E	Ego vehicle
C	Cut-in vehicle
L	Leading vehicle

Ego vehicle



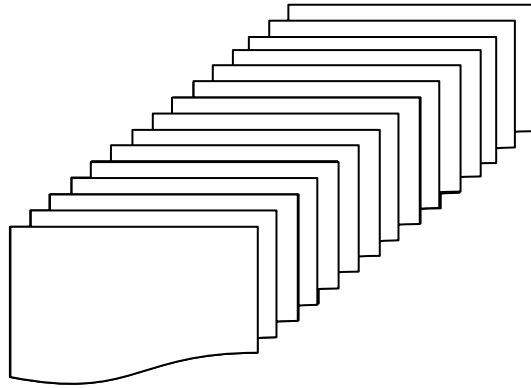
Cut in: Example of a concrete instance

- Deriving a concrete test scenario
 - Street dimensions
 - Relative positions of vehicles (road and other vehicles)
 - Velocities of vehicles
 - Changes of the dynamic parameters over time
- The derivation process should be systematic
 - This necessitates a formal description of scenarios



Standard risk computation

- List all hazards
- Derive all concrete instances
- Determine
 - Exposure
 - Criticality
 - Severity



- Sum up for overall risk

Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 100 km/h				
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h				
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 130 km/h				
...				
...				
...				
Sum				



Risk computation

- List all hazards
- Determine
 - Exposure
 - Criticality
 - Severity

Few valid data available

Can be measured by testing

Only rough models available

A very long list!

- Sum up for overall risk

Automation needed, but ingredients missing

Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 100 km/h		0.00		
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h		0.12		
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 130 km/h		0.00		
...				
...				
...				
Sum				



Formalization of scenarios: Description layers

- L1: Street layer:
 - Geometry, topology, material
- L2: infrastructure :
 - Boundaries, traffic signs, markings

manageable

- L3: Temporary modification of elements of L1 and L2 (example: installations of construction sites)

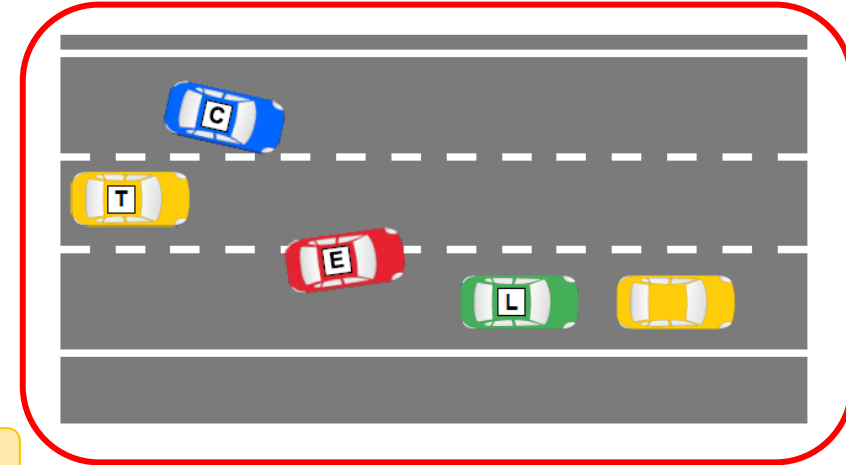
Irregular variations

- L4: Moving objects:
 - Types and specifics, dynamics

Focus

- L5: Environment conditions:
 - Weather, light

Very diverse



Layer definition after: Schuldt et al.
Effiziente systematische Testgenerierung für
Fahrerassistenzsysteme in virtuellen Umgebungen, AAET
2013. (further developed in PEGASUS)

Scene: snapshot of evolution

- **Traffic participants**

- **T, E, L**

- **Positions on the street**

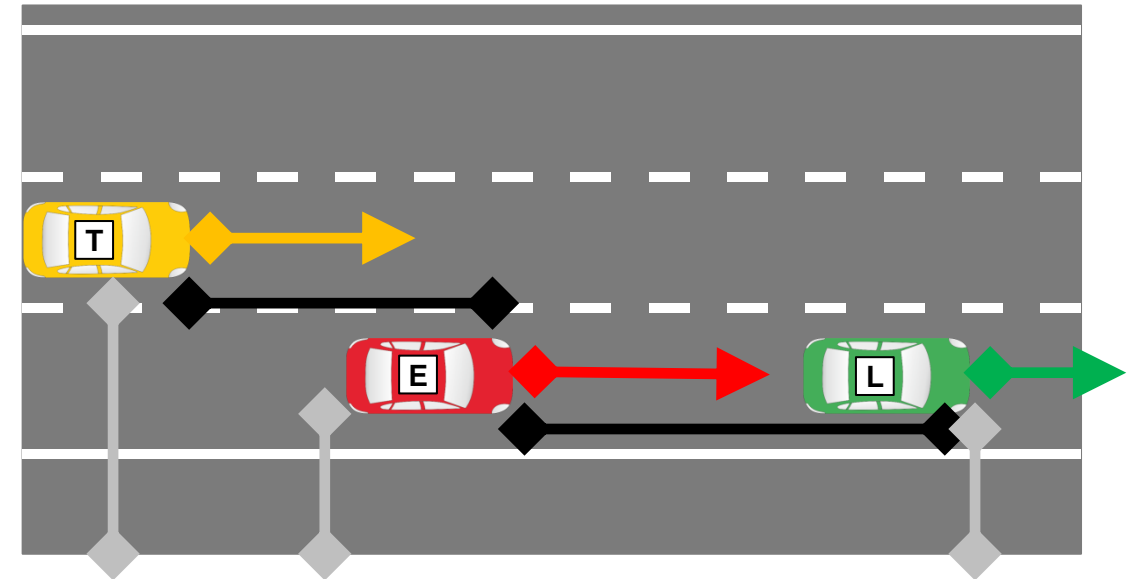
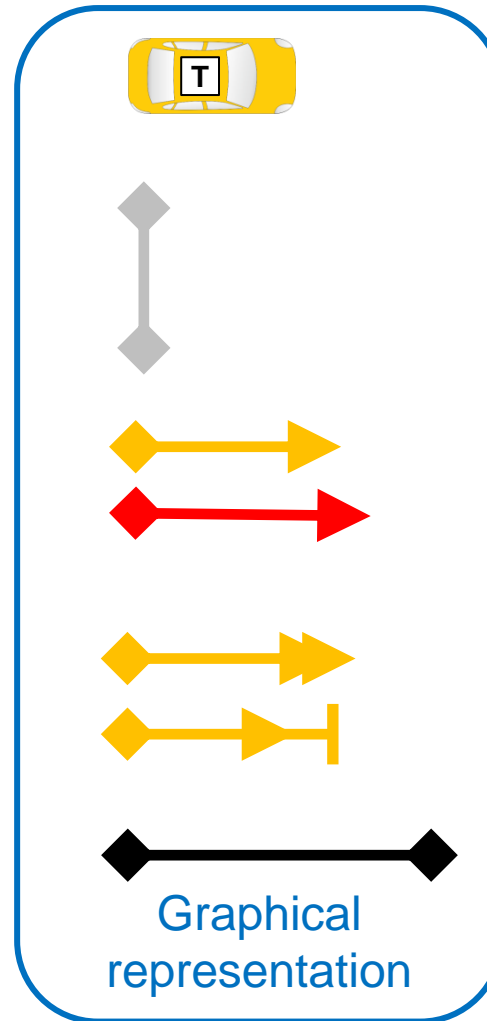
- Distance from road edge

- **Velocities**

- Acceleration
- Deceleration

- **Positions**

- (here: relative to **E**)



More complex: links
between scenes

Maneuver macros: Linking scenes to evolutions

Program-like descriptions of vehicle behavior

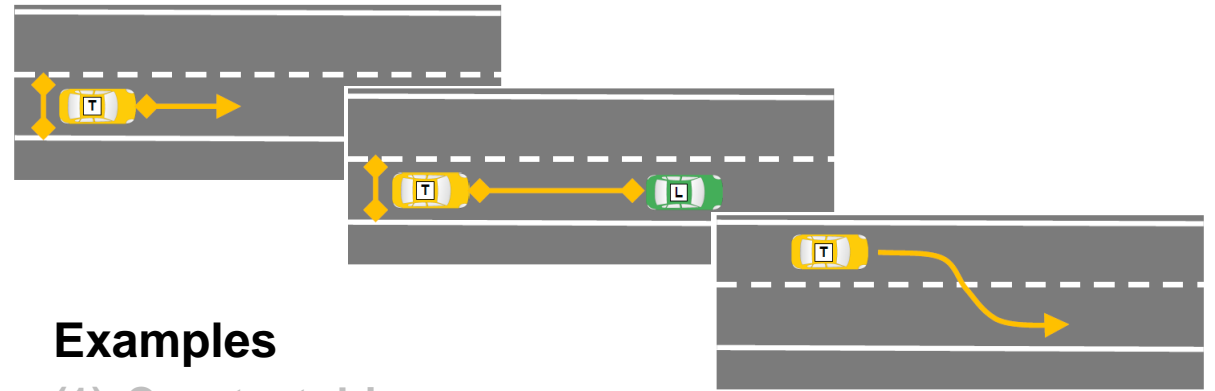
a. Geometry:

- Lateral position
- Discrete shape type: straight, sinusoidal, etc.
- Modifiers: distortions, deviations

b. Execution:

- time profile
- Completion condition (e.g.: time slot, space limitations)
- Absolute or relative to other traffic participants

c. End and exit conditions



Examples

(1) Constant drive

- Lane 1, straight, low lateral deviations
- constant velocity, low deviation
-

(2) Following

- Lane 1, straight, low lateral deviations
- Velocity adjusted on distance to lead vehicle
- Lane change of lead vehicle

(3) Lane change

- Lane 2, sinusoidal negative, low lateral deviations
- constant velocity, low deviation
- Completion of trajectory

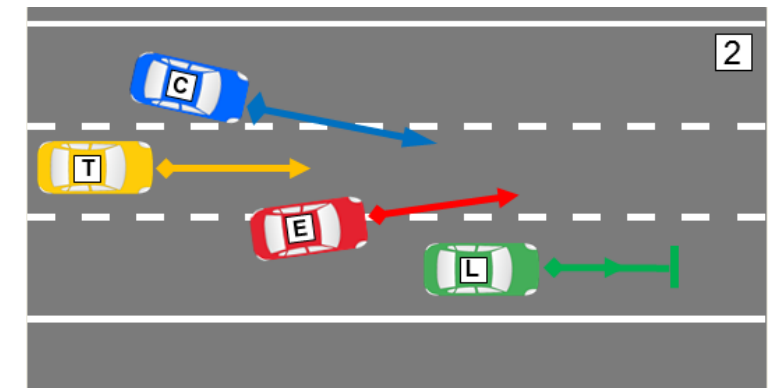
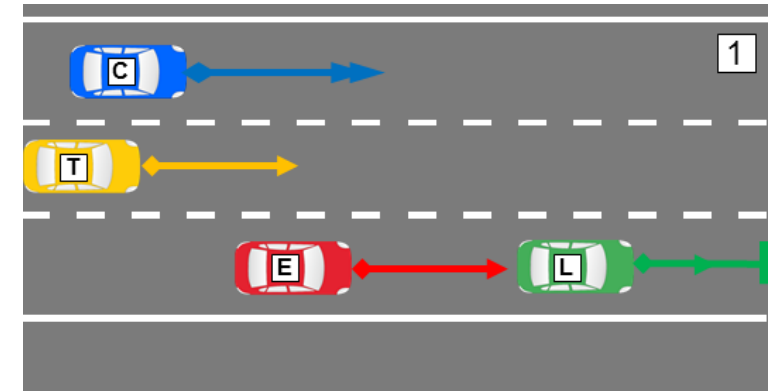
discrete parameter

numerical parameter



Example scenario: conflicting lane changes

0. The ego vehicle **E** follows **L** on the right lane
T is driving on the middle lane with the same velocity
1. **C** overtakes **T**,
L decelerates, which might provoke **E** to change lanes
2. **C** and **E** both move towards the middle lane



Example scenario: conflicting lane changes

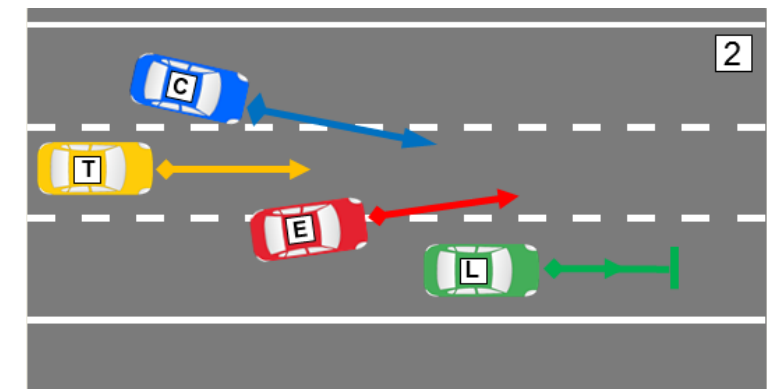
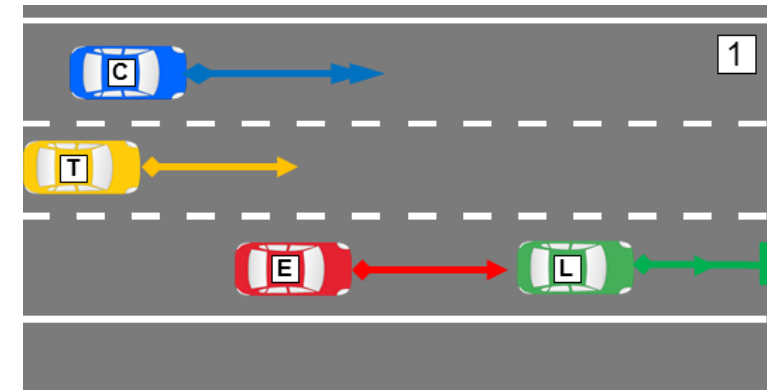
Programming the scenario with maneuver macros

0. **L**: constant drive
T: constant drive
C: lane following with goal constellation depending on (**C**, **T**, **E**)

1. **L**: lane following, decelerating
T: constant drive
C: lane following with goal constellation depending on (**C**, **T**, **E**)

C reaches goal constellation / **E** veers out

1. **L**: lane following, decelerating
T: constant drive
C: lane change



Precisely specifying the test space with logical scenarios

Shown

- **Building blocks of logical scenarios**

- Maneuver macros as elementary constituents
- Scenario definition by composing maneuver macros

- **Logical scenarios** are similar to programs

- Defining logical scenarios needs testing them (no reasonably complex program will be correct on first writing)

Comments

- The formalization may be seen as a domain-specific language
- The use of macros results in comprehensible definitions
- That maneuver macros capture real behaviours realistically can be validated on a reasonably small set of observation data.



Precisely specifying the test space with logical scenarios

Shown

• Building blocks of logical scenarios

- Maneuver macros as elementary constituents
- Scenario definition by composing maneuver macros

• Logical scenarios are similar to programs

- Defining logical scenarios needs testing them (no reasonably complex program will be correct on first writing)

• Coverage of the test space by complementary scenario spaces

- Manually manageable set of logical scenarios (though certainly large)

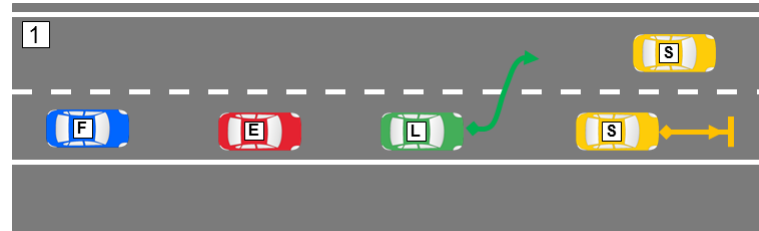
Comments

- The formalization may be seen as a domain-specific language
- The use of macros results in comprehensible definitions
- That maneuver macros capture real behaviours realistically can be validated on a reasonably small set of observation data.

Next

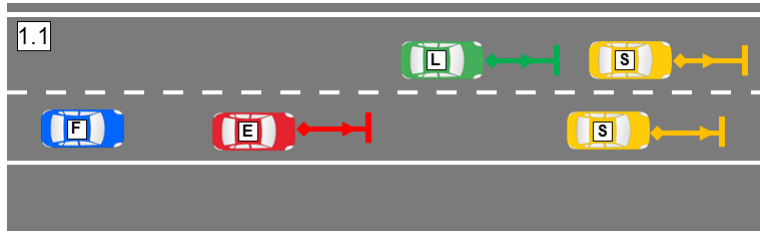


Scenario branching: Example

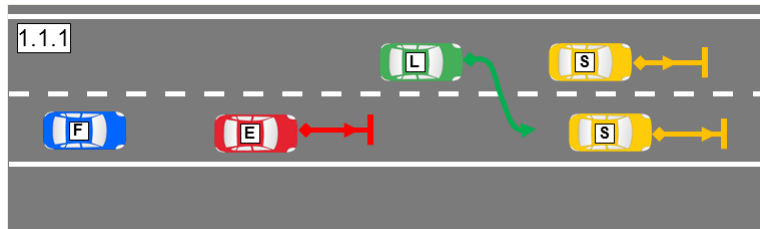


1. **E** follows **L** on the right lane
S decelerates
L changes lanes

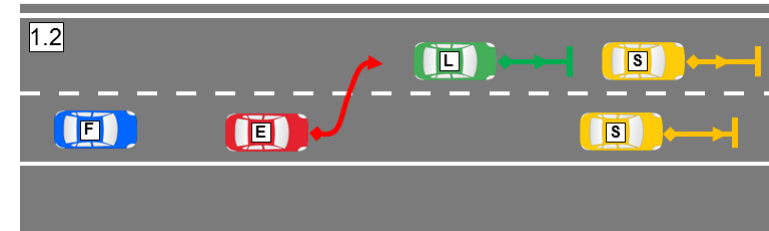
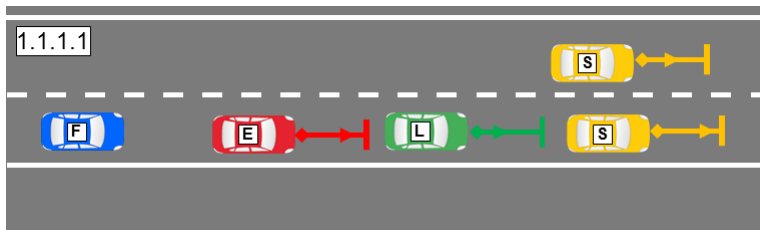
- 1.1 **E** decelerates
L decelerates



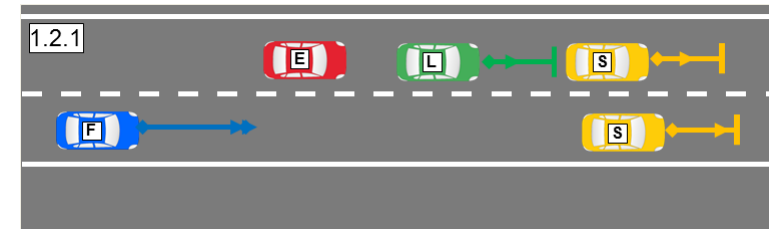
- 1.1.1 **L** changes back



- 1.1.1.1 **L** decelerates



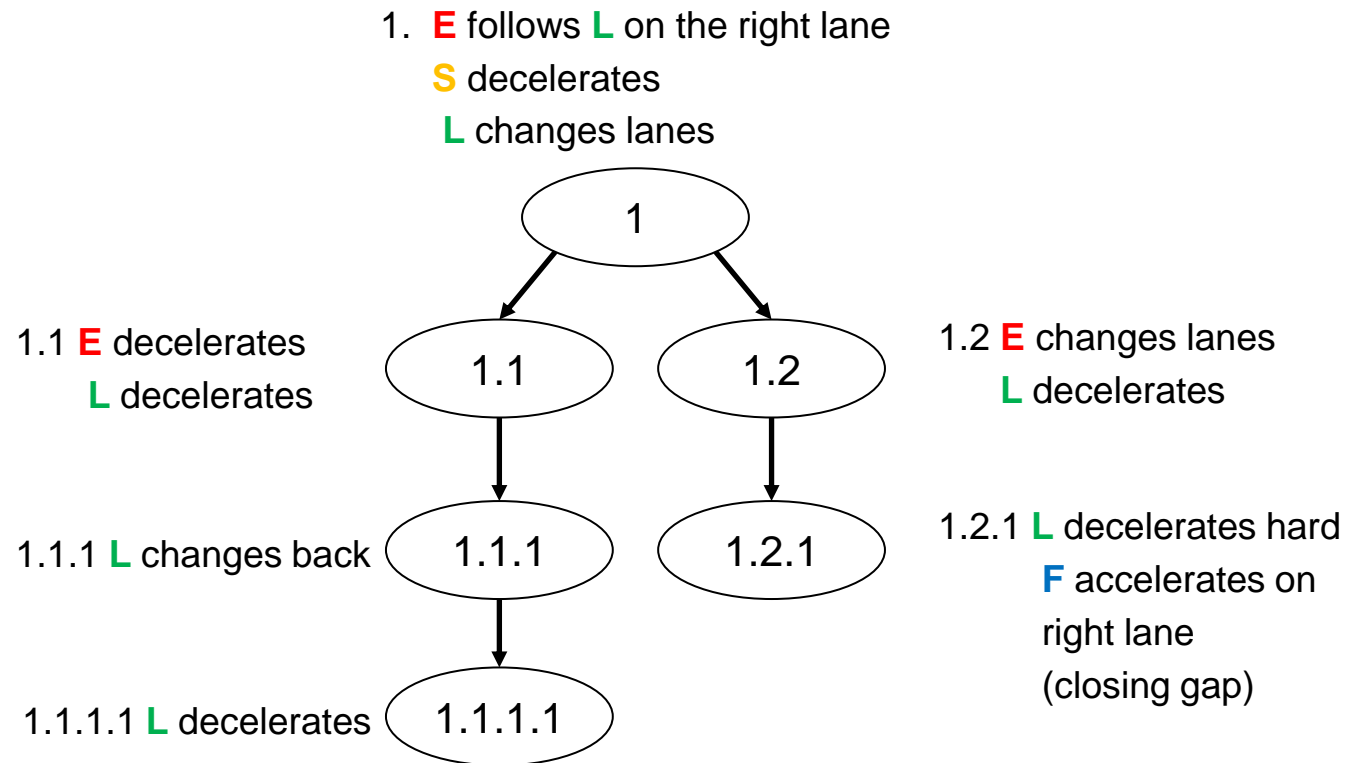
- 1.2 **E** changes lanes
L decelerates



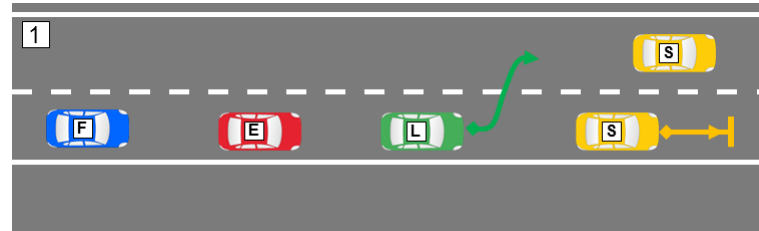
- 1.2.1 **L** decelerates hard
F accelerates on right lane
(closing gap)



Scenario branching: Tree structure

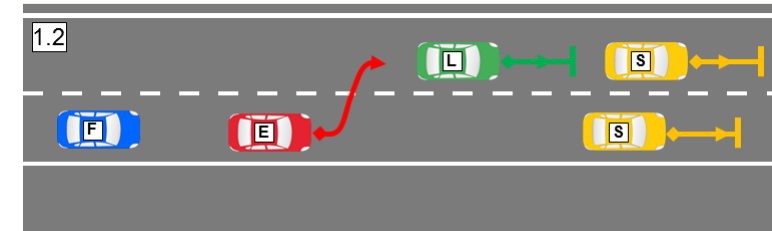
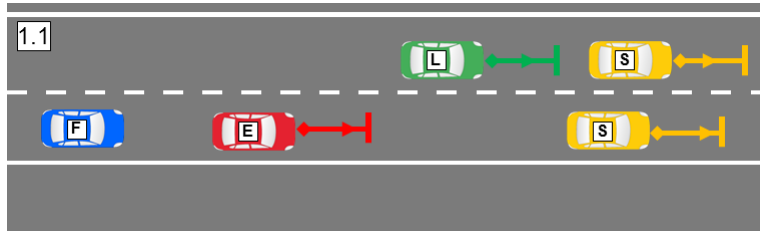


Scenario branching: Specification by two scenarios



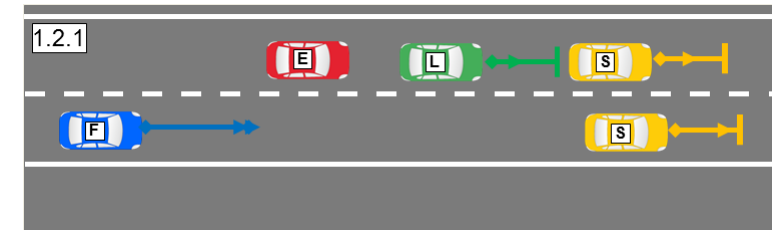
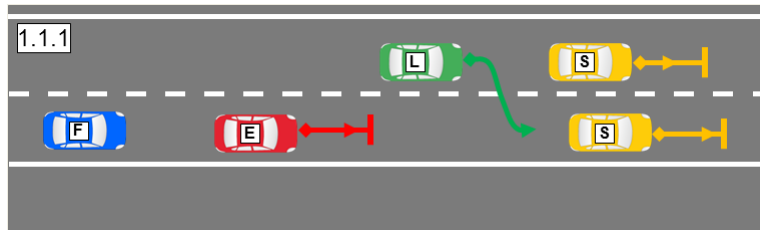
- 1. **E** follows **L** on the right lane
- S** decelerates
- L** changes lanes

- 1.1 **E** decelerates
- L** decelerates



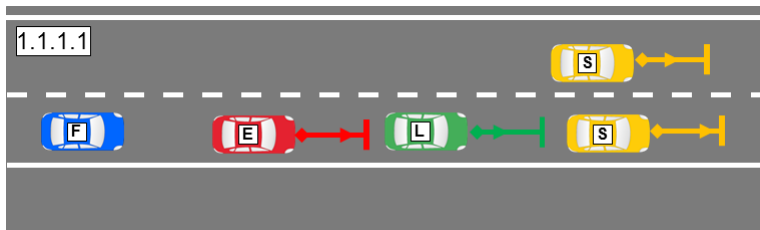
- 1.2 **E** changes lanes
- L** decelerates

- 1.1.1 **L** changes back

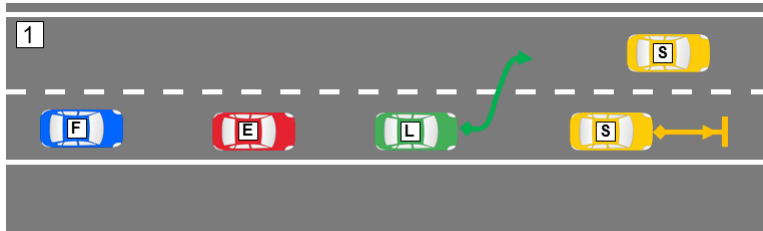


- 1.2.1 **L** decelerates hard
- F** accelerates on right lane (closing gap)

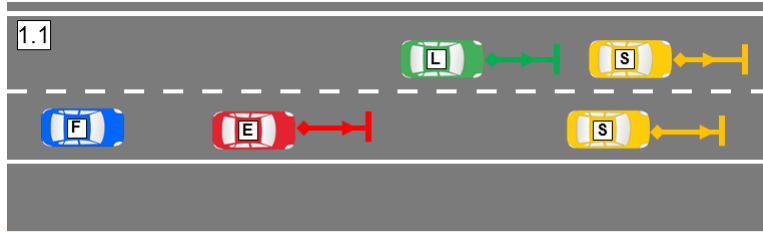
- 1.1.1.1 **L** decelerates



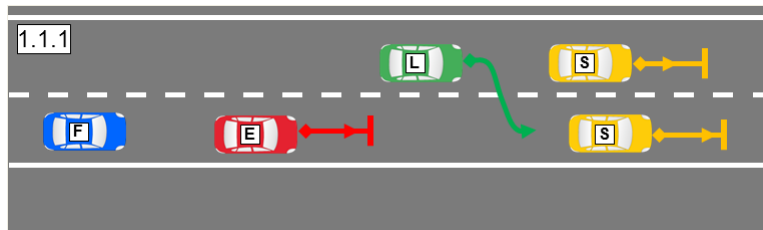
Scenario branching: Specification by two scenarios



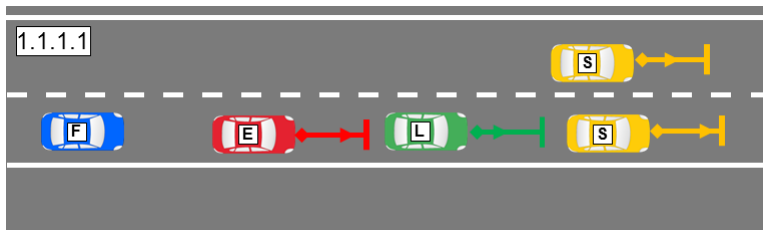
1.1 **E** decelerates
L decelerates



1.1.1 **L** changes back



1.1.1.1 **L** decelerates

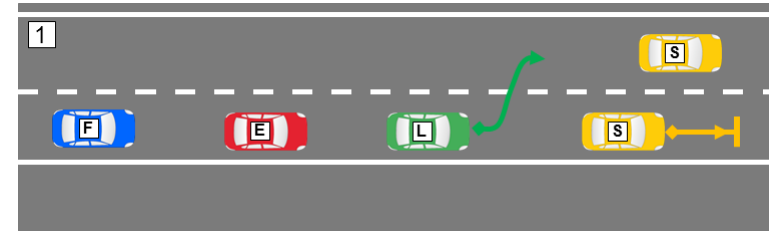


IF [**E** changes lanes] **THEN BREAK**

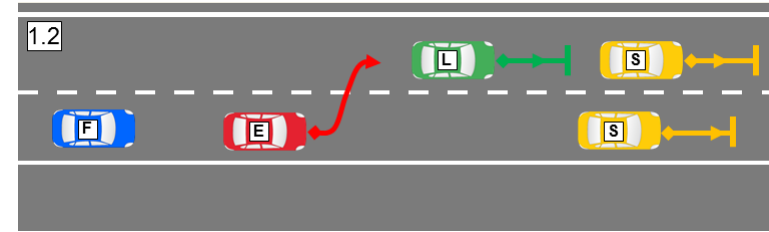


Scenario branching: Specification by two scenarios

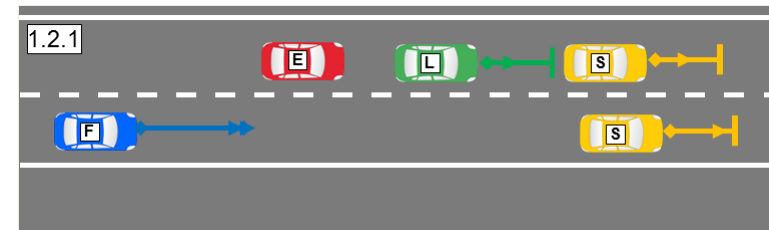
IF not([E changes lanes]) THEN BREAK



- 1. **E** follows **L**
- T** decelerates
- L** changes lanes



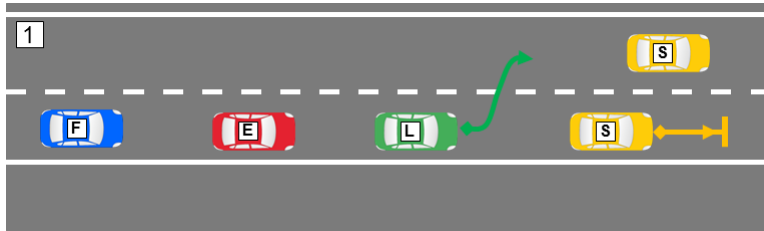
- 1.2 **E** changes lanes
- L** decelerates



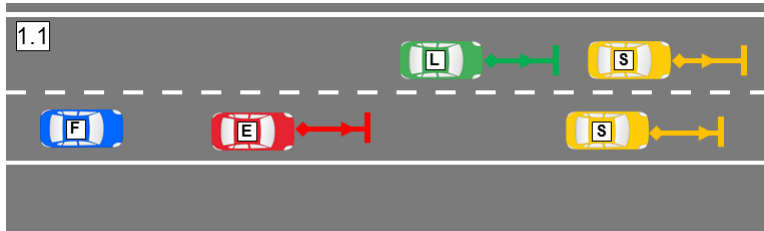
- 1.2.1 **L** decelerates hard
- F** accelerates on right lane (closing gap)

Scenario branching: Specification by two scenarios

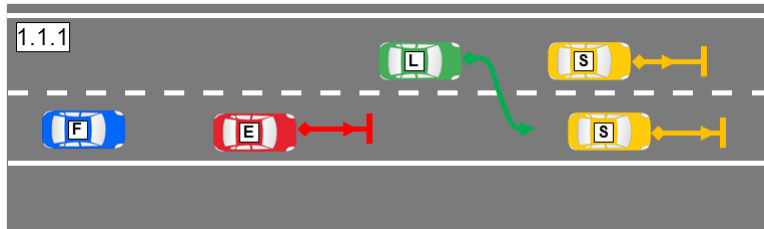
1. **E** follows **L**
T decelerates
L changes lanes



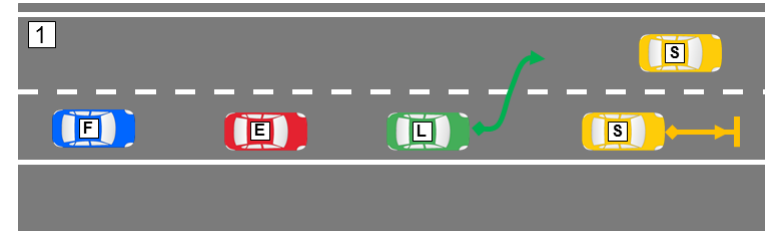
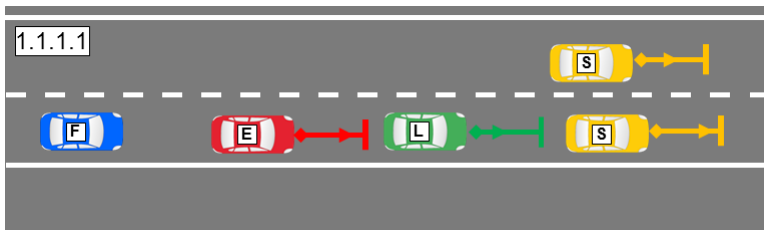
- 1.1 **E** decelerates
L decelerates



- 1.1.1 **L** changes back

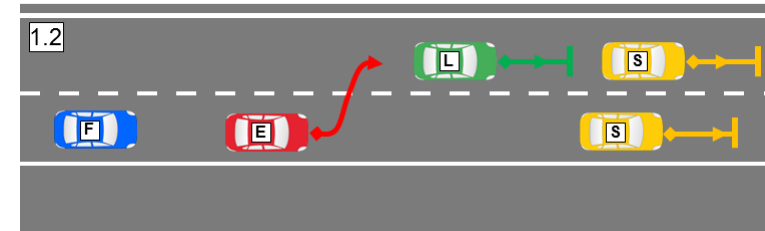


- 1.1.1.1 **L** decelerates

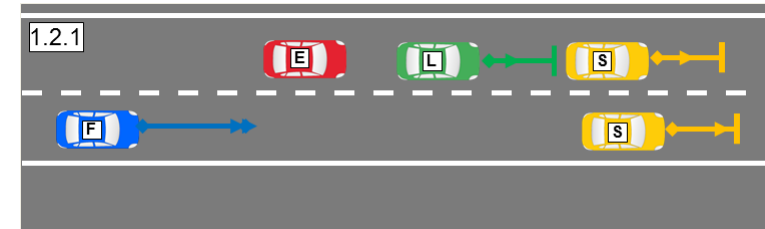


1. **E** follows **L**
T decelerates
L changes lanes

- 1.2 **E** changes lanes
L decelerates



- 1.2.1 **L** decelerates hard
F accelerates on right lane (closing gap)

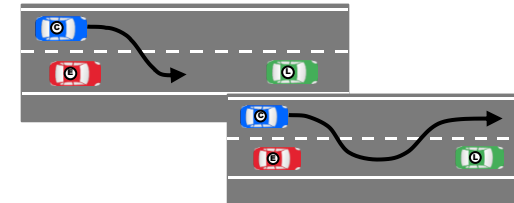


Different logical scenarios are distinguished by **different discrete actions** of **E** (and the other vehicles, of course).

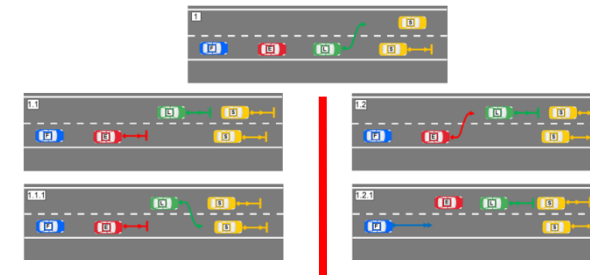
Not a formal definition - yet

Logical scenarios as test specification

1. Capture all dynamic evolutions in discrete event structures (functional scenarios)
2. Extract linear evolutions by splitting branches
3. Formalize linear evolutions in parameterized programs (logical scenarios)
4. Instantiate scenarios for complete set of test cases



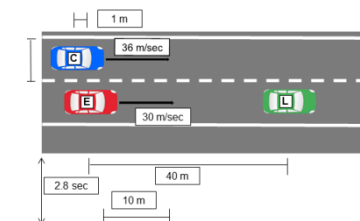
Functional scenarios



Linear scenarios

0. L: constant drive
 T: constant drive
 C: lane following with goal constellation depending on (C, T, E)
1. L: lane following, decelerating
 T: constant drive
 C: lane following with goal constellation depending on (C, T, E)

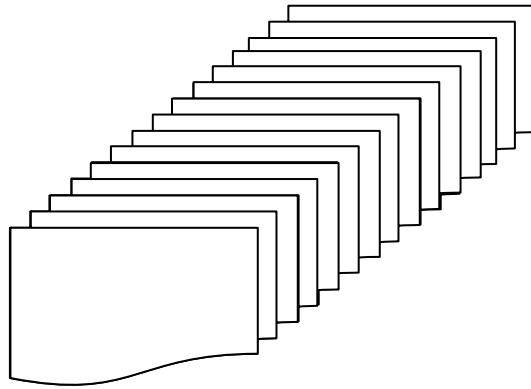
Logical scenarios



Concrete instances

Computing the risk

- List all hazards
- Determine
 - Exposure
 - Criticality
 - Severity

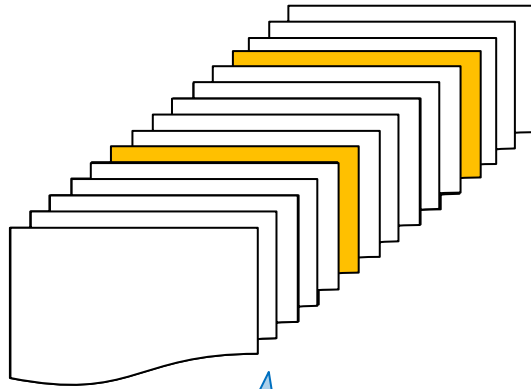


Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h				
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h				
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h				
...				
...				
...				
Sum				



Computing the risk

- List all hazards
- Determine
 - Exposure
 - **Criticality**
 - Severity



Formalized scenario descriptions enable automated test case generation

Splitting scenarios helps in keeping test cases disjoint

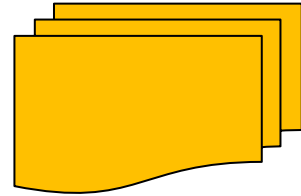
Determine values by automated simulation



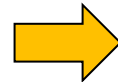
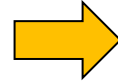
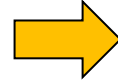
Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h		0.23		
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h		0.12		
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h		0.15		
...				
...				
...				
Sum				

Computing the risk

- List all hazards
- Determine
 - Exposure
 - **Criticality**
 - Severity



- Extract **relevant rows**



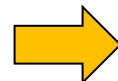
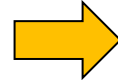
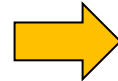
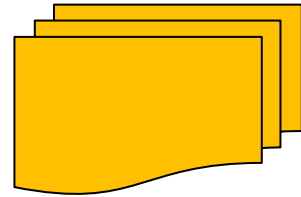
...

Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h		0.23		
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h		0.12		
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h		0.15		
...				
...				
...				
Sum				



Computing the risk

- List all hazards
- Determine
 - Exposure
 - Criticality
 - Severity
- Extract relevant rows
- Detailed analysis of risk in critical scenarios



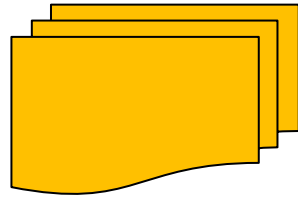
...

Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h	0.13	0.23	0.8	0.239
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h	0.02	0.12	1.3	0.003
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h	0.01	0.15	1.4	0.002
...				
...				
...				
Sum				

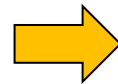


Computing the risk

- List all hazards
- Determine
 - Exposure
 - Criticality
 - Severity



- Extract relevant rows
- Detailed analysis of risk in critical scenarios
- Sum up for aggregated risk chart

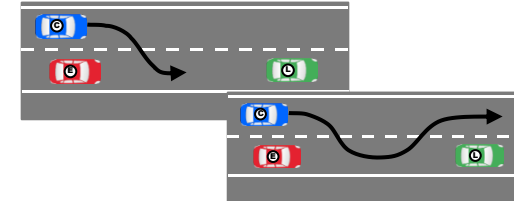


Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h	0.13	0.23	0.8	0.239
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h	0.02	0.12	1.3	0.003
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h	0.01	0.15	1.4	0.002
...				
...				
...				
Sum				



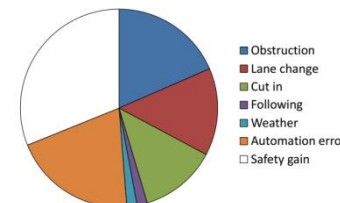
Conclusion

1. Capture all potentially critical evolutions in functional scenarios
2. Formalization of functional scenarios in precisely defined logical scenarios using maneuver macros
3. Identify all critical scenarios by systematic testing
4. Build the risk chart by analyzing and rating the critical scenarios



0. L: constant drive
 T: constant drive
 C: lane following with goal constellation depending on (C, T, E)
1. L: lane following, decelerating
 T: constant drive
 C: lane following with goal constellation depending on (C, T, E)

Hazard	E	C	S	Risk
Cut-in by vehicle entering highway Ego: 130 km/h, Cut-in-veh.: 85 km/h	0.13	0.23	0.8	0.239
...				
Cut-in by vehicle concealed by truck Ego: 130 km/h, Cut-in-veh.: 90 km/h	0.02	0.12	1.3	0.003
...				
Cut-in from left lane, decelerating Ego: 110 km/h, Cut-in-veh.: 115 km/h	0.01	0.15	1.4	0.002



Functional scenarios

Split scenarios

Logical scenarios

Concrete critical scenarios

Risk chart

Contact info

PD Dr. Hardi Hungar
German Aerospace Center
Institute of Transportation Systems
hardi.hungar@dlr.de

